In the claims:

1. (currently amended) A method for establishing a secure transmission channel from a user process running on a first partition of a first node partitioned into a plurality of partitions including the first partition, each partition having a corresponding operating system instance such that each partition is a separate virtual computer running on the first node, to a user process running on a second partition of a second node partitioned into a plurality of partitions including the second partition, each partition having a corresponding operating system instance such that each partition is a separate virtual computer running on the second node, the method comprising:

sending a key, identification of the first partition of the first node, and identification of the second partition of the second node from hardware of the first node to hardware of the second node, such that the key is inaccessible by all user processes running on the first node, in that none of the user processes are able to access the key, and unauthorized processes running on the first node are unable to send unauthorized messages through the hardware of the first node;

receiving the key, identification of the first partition of the first node, and identification of the second partition of the second node by the hardware of the second node;

verifying the identification of the first partition of the first node and the identification of the second partition of the second node by the hardware of the second node; and,

storing the key at the hardware of the second node, such that the key is inaccessible by all user processes running on the second node, in that none of the user processes are able to access the key,

wherein the hardware of the first hardware and the hardware of the second node establish a channel over which the user process running on the first partition of the first node and the user process running on the second partition of the second node are able to communicate, and

wherein the first and the second nodes are the same node.

2.-6. (cancelled)

7. (previously presented) The method of claim 1, wherein each of the hardware of the first node and the hardware of the second node comprises a connection management mechanism.

8. (previously presented) The method of claim 1, wherein verifying the identification of the first partition of the first node and the identification of the second partition of the second node by the hardware of the second node comprises verifying the identification of the first partition of the first node and the identification of the second partition of the second node in a channel state table accessible by the hardware of the second node and inaccessible by all the user processes of the second node, in that none of the user processes are able to access the channel state table.

9. (cancelled)

10. (previously presented) The method of claim 1, further comprising:

creating a message at the user process running on the second partition of the second node;

sending the message, the key, the identification of the first partition of the first node, and the identification of the second partition of the second node from the hardware of the second node to the hardware of the first node;

receiving the message, the key, the identification of the first partition of the first node, and the identification of the second partition of the second node by the hardware of the first node;

verifying the key at the hardware of the first node; and,

processing the message at the user process of the first node, where the key has been successfully verified at the hardware of the first node.

11. (currently amended) A computerized system comprising:

a plurality of nodes, each node having a plurality of partitions, each partition having a corresponding operating system instance such that the partition is a separate virtual computer running on the node, each partition having a plurality of user processes running thereon within the corresponding operating system instance of the partition;

a first secure connection management hardware mechanism at a first node of the plurality of nodes to maintain first keys for secure communication to first user processes running on the partitions of the first node from second user processes running on the partitions of a second node of the plurality of nodes, the first keys inaccessible by all user processes running on the partitions of the first node and running on the partitions of the second node in that none of the user processes are able to access the first keys, each first key used for secure communication to one of the first processes from one of the second user processes, and unauthorized processes running on the first node are unable to send unauthorized messages through the first secure connection management hardware of the first node; and,

a second secure connection management hardware mechanism at the second node to maintain second keys for secure communication to the second user processes from the first user processes, the second keys inaccessible by all user processes running on the partitions of the first node and running on the partitions of the second node in that none of the user processes are able to access the second keys, each second key used for secure communication to one of the second user processes from one of the first user processes,

wherein the first and the second secure connection management hardware mechanisms establish a channel over which the first user processes and the second user processes are able to communicate, and

wherein the first and the second nodes are the same node.

12. (previously presented) The system of claim 11, further comprising:

a first key table at the first node to store the first keys, the first key table accessible by the first secure connection management hardware mechanism but inaccessible by the first user processes in that none of the first user processes are able to access the first key table; and,

a second key table at the second node to store the second keys, the second key table accessible by the second secure connection management hardware mechanism but inaccessible by the second user processes in that none of the second user processes are able to access the second key table.

13. (previously presented) The system of claim 11, further comprising:

a first connection table at the first node and accessible by the first secure connection management hardware mechanism and the first user processes, the first connection table having a number of first entries, each first entry identifying one of the first user processes, one of the second user processes with which the one of the first user processes is securely communicating, and one of the partitions of the second node in which the one of the second user processes is running; and,

a second connection table at the second node and accessible by the second secure connection management hardware mechanism and the second user processes, the second connection table having a number of second entries, each second entry identifying one of the second user processes, one of the first user processes with which the one of the second user processes is securely communicating, and one of the partitions of the first node in which the one of the first user processes is running.

14. (previously presented) The system of claim 13, further comprising:

a first key table at the first node having a number of first key entries, each first key entry corresponding to a first entry of the first connection table and storing one of the first keys, the first key table accessible by the first secure connection management hardware mechanism but

inaccessible by the first user processes in that none of the first user processes are able to access the first key table; and,

a second key table at the second node having a number of second key entries, each second key entry corresponding to a second entry of the second connection table and storing one of the second keys, the second key table accessible by the second secure connection management hardware mechanism but inaccessible by the second user processes in that none of the second user processes are able to access the second key table.

15. (currently amended) An article comprising:

a computer-readable recordable data storage medium; and,

means in the medium for maintaining keys for secure communication to first processes running in a plurality of partitions of a first node from second processes running in a plurality of partitions of a second node, each partition having a corresponding operating system instance such that each partition is a separate virtual computer, the keys inaccessible by all user processes in that none of the user processes are able to access the keys, each key used for secure communication to one of the first user processes from one of the second user processes,

wherein unauthorized processes are unable to send unauthorized messages, and

wherein the first and the second nodes are the same node.

16. (previously presented) The article of claim 15, wherein the means in the medium is further for storing the keys in a key table inaccessible by all the user processes in that none of the user processes are able to access the key table.

17. (previously presented) The article of claim 15, wherein a connection table at the first node is accessible by the means in the medium and the first user processes, the connection table having a number of entries, each entry identifying one of the first user processes, one of the second user

processes with which the one of the first processes is securely communicating, and one of the partitions of the second node in which the one of the second user processes is running.

18. (previously presented) The article of claim 17, wherein a key table at the first node is accessible by the means in the medium but inaccessible by the first user processes in that none of the first user processes is able to access the key table, the key table having a number of key entries, each key entry corresponding to an entry of the connection table and storing one of the keys.

19.-26. (cancelled)